Vijeće
Europske unije

Bruxelles, 16. siječnja 2025.
(OR. en)

5426/25

CYBER 21
SAN 15

POPRATNA BILJEŠKA

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	15. siječnja 2025.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	COM(2025) 10 final
Predmet:	KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA Europski akcijski plan za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite

Za delegacije se u prilogu nalazi dokument COM(2025) 10 final.

Priloženo: COM(2025) 10 final

EUROPSKA
KOMISIJA

Bruxelles, 15.1.2025.
COM(2025) 10 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA

Europski akcijski plan za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite

1. Uvod

Sigurnosno okruženje EU-a brzo se mijenja zbog sve jačih hibridnih i kibernetičkih napada kojima je svrha destabilizirati naše društvo, nastojeći unijeti razdor i poremećaje, ali i profitirati od kibernetičkog kriminala. Europa zato mora hitno povećati pripravnost i otpornost na tu novu stvarnost, i to u svim sektorima i u skladu s pristupom koji obuhvaća „cijelo društvo" i „sve razine vlasti", na što se poziva u izvješću posebnog savjetnika predsjednice Europske komisije Saulija Niinistöa.

Sigurni i otporni zdravstveni sustavi temelj su EU-ova socijalnog modela. Bolnice i zdravstveni sustavi suočavaju se, međutim, sa sve većim prijetnjama, osobito od bandi koje ih zbog velike vrijednosti podataka o pacijentima, što uključuje elektroničke zdravstvene zapise, napadaju ucjenjivačkim softverom radi financijske koristi. Štoviše, zdravstveni je sektor u zadnje četiri godine, što obuhvaća i vrijeme pandemije bolesti COVID-19 kad je zdravstvena infrastruktura bila pod čestim kibernetičkim napadima, postao najnapadaniji sektoru u EU-u. Kibernetički napadi na bolnice i pružatelje zdravstvene zaštite izravno štete ljudima jer dovode do odgode medicinskih postupaka, paraliziraju hitni prijam i mogu, u ekstremnim slučajevima, prouzročiti gubitak života.

Te su opasnosti još i veće dok sektor prolazi vitalnu digitalnu transformaciju. Digitalno zdravstvo te upotreba i ponovna upotreba zdravstvenih podataka otvaraju put modelima zaštite koji su primjereniji potrebama i željama pacijenata jer sprečavaju pojavu bolesti ili omogućuju ranije liječenje. Integracija digitalnih alata i rješenja u kliničke postupke te upotreba i ponovna upotreba zdravstvenih podataka mogu biti temelj za bolje kliničke odluke i doprinijeti automatizaciji zdravstva te bržem i boljem liječenju. Digitalni alati, korištenje podataka i medicinski proizvodi, koji su često povezani s internetom i koje pokreće umjetna inteligencija, bitni su i za rješavanje problema kao što je nedostatak zdravstvenih radnika.

S druge strane, digitalni alati otvaraju nove potencijalne mete kibernetičkim kriminalcima. Uz to, kao što vidimo na primjeru aktualnog agresivnog rata Rusije protiv Ukrajine, od napada na zdravstvene ustanove ne prezaju ni određeni državni akteri. Zbog toga je taj sektor potencijalna meta kibernetičkih napada u okviru većih hibridnih kampanja. Ti napadi ne samo da ugrožavaju sigurnost pacijenata nego i slabe povjerenje javnosti u zdravstvenu infrastrukturu, a trošak oporavka od njih je znatan. Osim za zaštitu od kibernetičkih napada, otporna i sigurna digitalna infrastruktura ključna je i za potporu provedbi i potpunom uvođenju europskog prostora za zdravstvene podatke[1].

Dakle, kako je istaknula predsjednica von der Leyen u svojim političkim smjernicama za Komisiju za razdoblje 2024. – 2029.[2], vrijeme je da povećamo i ujednačimo kibernetičku sigurnost i otpornost europskih bolnica i pružatelja zdravstvene zaštite. Ovaj akcijski plan odgovor je na hitnost situacije i jedinstvene prijetnje kojima je taj sektor izložen. Kako za probleme kibernetičke sigurnosti u zdravstvu nema jednostavnog, čudotvornog lijeka, u planu se poziva na poboljšanje prevencije i pripravnosti te na usklađenije poimanje solidarnosti uz iskorištavanje stručnosti europskog sektora kibernetičke sigurnosti. Akcijski plan tako slijedi EU-ov pristup sigurnosti koji će biti podrobnije razrađen i formaliziran u skoroj europskoj strategiji unutarnje sigurnosti, u kojoj će se definirati sveobuhvatan odgovor za suočavanje sa

[1] https://www.consilium.europa.eu/hr/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/.
[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_hr.

svim prijetnjama unutarnjoj sigurnosti, pri čemu će u prvom planu biti sposobnost predviđanja prijetnji, sprečavanja štete i zaštite ljudi djelovanjem na svim razinama i za cijelo društvo.

Zdravstveni sektor obuhvaća velik broj subjekata i aktera, uključujući bolnice, klinike, domove za skrb, centre za rehabilitaciju i razne pružatelje zdravstvene zaštite, uz farmaceutski, medicinski i biotehnološki sektor, proizvođače medicinskih proizvoda i zdravstvene istraživačke ustanove. Akcijski plan primarno se bavi kibernetičkom sigurnosti bolnica i pružatelja zdravstvene zaštite, kojima se smatraju sve fizičke ili pravne osobe ili drugi subjekti koji zakonito pružaju zdravstvenu zaštitu na državnom području države članice[3]. Bolnice i pružatelji zdravstvene zaštite u međuovisnom su odnosu s drugim zdravstvenim subjektima i neposredno rade s ljudima. Mjerama za povećanje kibernetičke sigurnosti bolnica i pružatelja zdravstvene zaštite trebali bi se također smanjiti rizici koji utječu na širi lanac opskrbe i ekosustav, a izvor su im, primjerice, subjekti koji koriste zdravstvene podatke za istraživanje i strojno učenje ili koji proizvode medicinske proizvode, osobito digitalne medicinske proizvode koji se povezuju s internetom ili drugim uređajima („internet stvari").

Zaštita zdravstvenih sustava prvenstveno je u nacionalnoj nadležnosti, no zdravstvo je i svrstano u kritične sektore u Direktivi o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS 2)[4]. Kibernetički kriminalci i drugi prijeteći akteri operiraju preko državnih granica, a i problemi kibernetičke sigurnosti s kojima se suočavaju zdravstvene organizacije slični su u svim državama članicama. Suradnja na europskoj razini korisna je za razmjenu i širu primjenu najboljih praktičnih pristupa na razini EU-a i na nacionalnoj razini. Zato se u akcijskom planu predlažu mjere i koordinacija na razini EU-a, a države članice pozivaju se da poduzmu korake da pomognu sektoru zdravstvene zaštite i širem zdravstvenom ekosustavu.

Središnje mjesto u akcijskom planu ima razvoj sektorskih kapaciteta za **sprečavanje** kibernetičkih sigurnosnih incidenata jer uvijek je bolje spriječiti nego liječiti. Drugo, u akcijskom planu detaljno su opisane mjere za poboljšanje dijeljenja informacija o kibernetičkoj sigurnosti i sposobnosti za **otkrivanje** kibernetičkih prijetnji, što omogućuje brže reakcije. Treće, u njemu se navode mjere za bolji **odgovor** na incidente i **oporavak** od njih. Na kraju, u planu su predviđeni načini za **odvraćanje** aktera kibernetičkih prijetnji od pokretanja napada na zdravstvene sustave u Europi.

Akcijski plan provodit će se u suradnji s pružateljima zdravstvene zaštite i širim zdravstvenim ekosustavom, državama članicama te zajednicom za kibernetičku sigurnost. Suradnički pristup bitan je da se najdjelotvornije mjere razrade i dorade tako da koristi od njih mogu imati svi ključni pružatelji zdravstvene zaštite u Europi i zato će se uz ovu Komunikaciju pokrenuti cjelovito savjetovanje s dionicima, sektorom i državama članicama. Za kibernetičku sigurnost važna je i međunarodna suradnja jer kibernetičke prijetnje ne poznaju granice i međusobno su povezane. Slične su kibernetičke sigurnosne prijetnje prisutne i u zemljama kandidatkinjama i susjednim zemljama te u drugim strateškim partnerskim zemljama EU-a, a to na koncu može ugroziti sigurnost kritične infrastrukture u EU-u. Zato

[3]Članak 3. točka (g) Direktive 2011/24/EU Europskog parlamenta i Vijeća o primjeni prava pacijenata u prekograničnoj zdravstvenoj skrbi, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32011L0024.

[4] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (Direktiva NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

će biti važno da se iskustva iz provedbe akcijskog plana iskoriste i u suradnji EU-a sa zemljama proširenja i drugim partnerskim zemljama, ovisno o stupnju prijetnji kojima su izložene.

2. Pitanje kibernetičke sigurnosti bolnica i pružatelja zdravstvene zaštite

Kibernetičke prijetnje zdravstvenom sektoru

Kibernetički napadi u porastu su u svijetu i unutar EU-a, a prijetnje su sve složenije i dinamičnije. Pomaci u umjetnoj inteligenciji daju kriminalnim i zlonamjernim akterima moćne alate kojima mogu povećati preciznost i uspješnost svojih operacija, ali isto tako unapređuju mogućnosti kibernetičke obrane jer omogućuju da se protiv napada djeluje automatizirano i u stvarnom vremenu.

Ucjenjivački softver i dalje je jedan od glavnih problema kibernetičke sigurnosti u EU-u i svijetu. U jednom se izvješću procjenjuje se da će do 2031. prouzročiti svjetski godišnji trošak veći od 250 milijardi EUR[5]. Kriminalci koji koriste ucjenjivački softver ne samo da šifriraju podatke žrtava radi otkupnine nego i sve češće odaju osjetljive informacije kako bi izvršili dodatni pritisak. Softverske i hardverske ranjivosti još su jedan velik problem: prema Agenciji Europske unije za kibersigurnost (ENISA)[6], zdravstvo je sektor koji je izvijestio o najvećem broju sigurnosnih incidenata zbog tih ranjivosti[7]. Među ostalim sve brojnijim prijetnjama su distribuirani napadi uskraćivanjem usluge (DDoS), odnosno preopterećivanje ciljanog sustava velikom količinom prometa kako bi postao nedostupan pravim korisnicima[8].

Zdravstveni sektor suočava se sa sličnim trendovima u kibernetičkim prijetnjama, pri čemu se osobito ističu napadi ucjenjivačkim softverom. Prema ENISA-i, u razdoblju 2021. – 2023. ucjenjivački softver korišten je u 54 % analiziranih kibernetičkih sigurnosnih incidenata u zdravstvenom sektoru. U 83 % napada motiv je bio financijski, zbog velike vrijednosti zdravstvenih podataka, a 10 % napada bilo je ideološki motivirano[9]. Slično tome, u izvješću Komisije iz 2024. utvrđeno je da su napadi ucjenjivačkim softverom činili 71 % napada s posljedicama na liječenje pacijenata, kao što su odgoda liječenja i dijagnoze i otežan pristup hitnoj pomoći[10]. Napadi ucjenjivačkim softverom mogu osobito poremetiti

[5] Cybersecurity Ventures (1. lipnja 2024.): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Dostupno na https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (Akt o kibersigurnosti), https://eur-lex.europa.eu/eli/reg/2019/881/oj/hrv.

[7] *ENISA Threat Landscape*: *Health Sector* (srpanj 2023.).

[8] *ENISA Threat Landscape 2024*.

[9] *ENISA Threat Landscape*: *Health Sector* (srpanj 2023.). U izvješću su analizirani pružatelji zdravstvene zaštite i druge vrste organizacija, uključujući one koje provode istraživanja povezana sa zdravljem, subjekti koji proizvode određene proizvode povezane sa zdravljem, zdravstvena tijela, organizacije zdravstvenog osiguranja, odgojno-rehabilitacijske ustanove i pružatelji socijalnih usluga. Dostupno na https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Europska komisija: Zajednički istraživački centar, Reina, V. i Griesinger, C., Kibernetička sigurnost u zdravstvenom i medicinskom sektoru – studija o dostupnim dokazima o posljedicama kibernetičkih incidenata u zdravstvenoj zaštiti na zdravlje pacijenata (*Cyber security in the health and medicine sector – A study on available evidence of patients health*

pružanje zdravstvenih usluga i tako ugroziti sigurnost pacijenata. Uz to, često su povezani s povredama podataka o pacijentima[11], koje se nerijetko odnose na osjetljive zdravstvene podatke i krše temeljno ljudsko pravo na zaštitu osobnih podataka.

U isto vrijeme zbog sve digitaliziranije zdravstvene zaštite raste površina napada. Prema Izvješću o stanju digitalnog desetljeća 2024., u prosjeku 79 % građana EU-a ima internetski pristup svojim elektroničkim zdravstvenim zapisima u primarnoj zdravstvenoj zaštiti[12]. Elektronički zdravstveni zapisi, klinički informacijski sustavi, bolnički sustavi tijeka rada, informatički sustavi za obradu povrata troškova liječenja, sustavi za medicinsko snimanje i medicinski proizvodi koji se koriste u dijagnostičke svrhe ili za praćenje pacijenata primjeri su digitalnih alata koji mogu imati važnu ulogu u povećanju učinkovitosti i uspješnosti zdravstvenog sektora, ali su i potencijalne mete kibernetičkih napada. Riziku od tih napada osobito su izložene specifične aktivnosti zdravstvene zaštite kao intenzivna njega i radiološko snimanje ili područja medicine kao onkologija i kardiologija, koje uvelike ovise o digitalnim uređajima. Uz to, nedostaci u lancu opskrbe mogu rezultirati nabavom proizvoda nedostatne kibernetičke sigurnosti i tako pogoršati postojeće opće rizike.

Primjerice, za vrijeme pandemije bolesti COVID-19 napad ucjenjivačkim softverom paralizirao je velike dijelove irskog sustava zdravstvene zaštite zbog čega su na jutro incidenta u 31 od 54 bolnice otkazane barem neke usluge[13]. Zdravstvene službe morale su raditi s papirnatom dokumentacijom, što ih je usporilo. Napad je bio izveden *phishing* e-porukom sa zlonamjernim prilogom[14]. Incident je ukazao na potencijal širenja kibernetičkih napada na razne sustave, a time i na važnost zaštite cjelokupne površine napada bilo koje organizacije za zdravstvenu zaštitu. Također je upozorio na važnost temeljne kulture kibernetičke higijene i kibernetičke sigurnosti u svim organizacijama.

Zrelost kibernetičke sigurnosti bolnica i pružatelja zdravstvene zaštite

Zdravstveno okruženje u EU-u veoma je raznoliko. Bolnice i drugi pružatelji zdravstvene zaštite u državama članicama znatno se razlikuju po vlasništvu, strukturi i veličini. U nekim se slučajevima zdravstvenom zaštitom upravlja centralizirano na nacionalnoj razini, a u drugima na regionalnoj i lokalnoj razini, dok pružatelji zdravstvene zaštite mogu biti u javnom ili privatnom vlasništvu. Razlike mogu postojati i unutar iste zemlje, primjerice kad se regije znatno socioekonomski i teritorijalno razlikuju, i to stvara složenu situaciju. Tako složeno zdravstveno okruženje može biti slaba točka u velikim zdravstvenim krizama zbog zaraznih bolesti, kao što je bila pandemija bolesti COVID-19, ali i kod drugih zdravstvenih rizika, primjerice onih povezanih s klimatskim promjenama. Na kraju, znatne razlike i rascjepkanost postoje i u stupnju digitaliziranosti i uvođenju tehnologije u rad pružatelja

consequences from cyber incidents in healthcare settings), Ured za publikacije EU-a, 2024., https://data.europa.eu/doi/10.2760/693487.

[11] Prema ENISA-inu izvješću *Threat Landscape* u zdravstvenom su sektoru povrede ili krađe podataka potvrđene u 43 % analiziranih incidenata s ucjenjivačkim softverom.

[12] Izvješće o stanju digitalnog desetljeća za 2024.

[13] Health Service Executive (2021): *Conti cyber attack on the HSE: Independent Post Incident Review*.

[14] Health Service Executive: *Cyber-attack and HSE response*. Dostupno na https://www2.hse.ie/services/cyber-attack/what-happened/.

zdravstvene zaštite. Tu složenost dobro ilustrira činjenica da nedostupnost usluga zbog kibernetičkog sigurnosnog incidenta može prouzročiti ozbiljnu štetu pacijentima čak i u malim zdravstvenim ustanovama, uključujući klinike ili hitne medicinske službe čije su usluge važne relativno malom broju korisnika.

Prema ENISA-inu Izvješću o stanju kibernetičke sigurnosti u Uniji za 2024.[15] kibernetička sigurnost zdravstvenog sektora EU-a umjereno je zrela, ali postoje znatne razlike među zdravstvenim subjektima u Europi. Manjkavosti su vidljive u važnim područjima kao što su dostatnost ljudskih resursa, znanje organizacija o vlastitim lancima opskrbe informacijskom i komunikacijskom tehnologijom (IKT) te ažuriranje sigurnosnih funkcionalnosti u proizvodima. Sektor ima poteškoća s osnovnom kibernetičkom higijenom i temeljnim sigurnosnim mjerama, što ilustrira činjenica da gotovo sve anketirane zdravstvene organizacije imaju problema s procjenom kibernetičkih sigurnosnih rizika, a gotovo ih polovina nikad nije provela analizu rizika[16].

Za kibernetičku sigurnost bolnica važan je problem i to što su one sjecišta informacijske tehnologije i operativne tehnologije, čiji se sigurnosni prioriteti razlikuju u pogledu povjerljivosti, dostupnosti i pouzdanosti, a povreda u jednom području može utjecati na drugo. U ENISA-inu Izvješću o stanju kibernetičke sigurnosti u Uniji za 2024. zatim je istaknuto da zdravstveni sektor ne postiže odgovarajuće rezultate kad je riječ o sigurnosti IKT proizvoda i postupaka koje primjenjuje zato što su zdravstveni subjekti, uređaji i proizvodi vrlo raznoliki.

Ta raznolikost, u kombinaciji s različitim stupnjevima poznavanja kibernetičke sigurnosti među bolničkim osobljem i upravom, komplicira postizanje kibernetičke sigurnosti zdravstvenih sustava. Primjerice, prema Eurobarometru o kibernetičkim vještinama za 2024. samo je 25 % anketiranih poduzeća u zdravstvu, obrazovanju i socijalnoj skrbi u prethodnih 12 mjeseci organiziralo osposobljavanje ili informiranje na temu kibernetičke sigurnosti[17]. Nužno je raditi na razvoju kulture osviještenosti o kibernetičkoj sigurnosti među zdravstvenim djelatnicima koji rade izravno s ljudima. Naprimjer, rotacije osoblja, korištenje zajedničkih radnih stanica, loše upravljanje autentifikacijom i upotreba prenosivih medija dodatni su izvori nedostataka koji utječu na kibernetičku sigurnost pružatelja zdravstvene zaštite[18].

U mnogim su slučajevima informacijske i operativne tehnologije barem djelomično izdvojene vanjskim dobavljačima. Eurobarometar za 2024. pokazao je da je udio poduzeća koja izdvajaju barem neke aspekte svoje kibernetičke sigurnosti najviši u zdravstvu, obrazovanju i socijalnoj skrbi: to radi 57 % anketiranih poduzeća[19]. Slično tome, prisutan je jak trend prelaska na računalstvo u oblaku, potaknut potrebom za

---

[15] ENISA: *2024 Report on the State of Cybersecurity in the Union* (rujan 2024.). Dostupno na https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[16] *ENISA Threat Landscape*: *Health Sector* (srpanj 2023.). Dostupno na https://www.enisa.europa.eu/publications/health-threat-landscape.

[17] Brza anketa Eurobarometra 547 o kibernetičkim vještinama (svibanj 2024.). Dostupna na: https://europa.eu/eurobarometer/surveys/detail/3176.

[18] Panacea – *People-centric cybersecurity in healthcare* (2021.): *White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres*.

[19] Brza anketa Eurobarometra 547 o kibernetičkim vještinama (svibanj 2024.). Dostupna na: https://europa.eu/eurobarometer/surveys/detail/3176.

skalabilnom pohranom i upravljanjem podacima, troškovnom učinkovitošću, boljom suradnjom i potporom naprednim tehnologijama kao što su umjetna inteligencija i internet medicinskih stvari. U 2022. 58 % zdravstvenih organizacija koristilo je neku digitalnu zdravstvenu platformu koja se temelji na oblaku[20]. Ta promjena može znatno povećati učinkovitost, no ona za sobom povlači i rizike koji iziskuju utemeljene odluke o nabavi i sigurnoj konfiguraciji.

No iznad svih tih problema nadvija se pitanje izgradnje kapaciteta i financiranja. Financiranje kibernetičke sigurnosti u zdravstvenom sektoru je ograničeno te je i dalje univerzalni problem u cijelom EU-u[21]. Uz to, problemi s financiranjem događaju se u uvjetima kad je stanovništvo sve starije i očekuje se da će to u idućim desetljećima stvoriti velike proračunske pritiske na europske zdravstvene sustave.

Nastavak upotrebe zastarjelih alata i naslijeđenih sustava, ograničeni resursi za sprečavanje incidenata ili odgovor na njih te manjkava zrelost kibernetičke sigurnosti često su posljedica nedovoljnog financiranja. Bolnice neprestano moraju održavati ravnotežu između suvremene sigurne i digitalne infrastrukture i drugih nužnih ulaganja za poboljšanje skrbi o pacijentima, kao što su zapošljavanje liječnika i drugih zdravstvenih radnika, uvođenje novih načina dijagnostike i liječenja te nabava opreme. Prema ENISA-i[22], po udjelu potrošnje za informacijsku sigurnost u ukupnoj potrošnji za informacijsku tehnologiju zdravstveni je sektor s medijanom od 8,3 % tek sedmi od 12 analiziranih sektora.

3. Europski potporni centar za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite

Okvir EU-a za kibernetičku sigurnost nudi razne instrumente koje bi trebalo iskoristiti za povećanje sigurnosti i otpornosti bolnica i pružatelja zdravstvene zaštite. Kako bi se riješili navedeni mnogobrojni problemi, potrebno je razviti jedinstven, strateški pristup na razini EU-a kojim bi se objedinili potrebni resursi, stručno znanje i alati za uspješno suzbijanje kibernetičkih prijetnji. Da bi se pružateljima zdravstvene zaštite u EU-u pomoglo da učvrste obranu nužno je imati cjelovit pregled, kao i bolje planiranje i koordinaciju. U tu je svrhu najprimjerenije da ENISA, u okviru svojeg mandata[23] da štiti i podupire kritičnu infrastrukturu EU-a, unutar svoje organizacije osnuje namjenski **Europski potporni centar za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite**[24].

Potporni centar trebao bi postupno **izraditi sveobuhvatan katalog usluga u skladu s potrebama bolnica i pružatelja zdravstvene zaštite**, u kojem će u glavnim crtama biti prikazane dostupne usluge za pripravnost, prevenciju, otkrivanje i odgovor. U suradnji s tijelima država članica i oslanjajući se na iskustva bolnica i pružatelja zdravstvene zaštite trebao bi izraditi lako dostupan i korisnicima prilagođen repozitorij svih dostupnih instrumenata na europskoj, nacionalnoj i regionalnoj razini. Svoje aktivnosti

[20] ENISA: *NIS Investments Report 2022* (studeni 2022.). Dostupno na https://www.enisa.europa.eu/publications/nis-investments-2022.

[21] Organizacija i pružanje zdravstvenih usluga i medicinske skrbi u nacionalnoj su nadležnosti u skladu s člankom 168. Ugovora o funkcioniranju Europske unije, a financiranje zdravstvenih sustava razlikuje se među državama članicama.

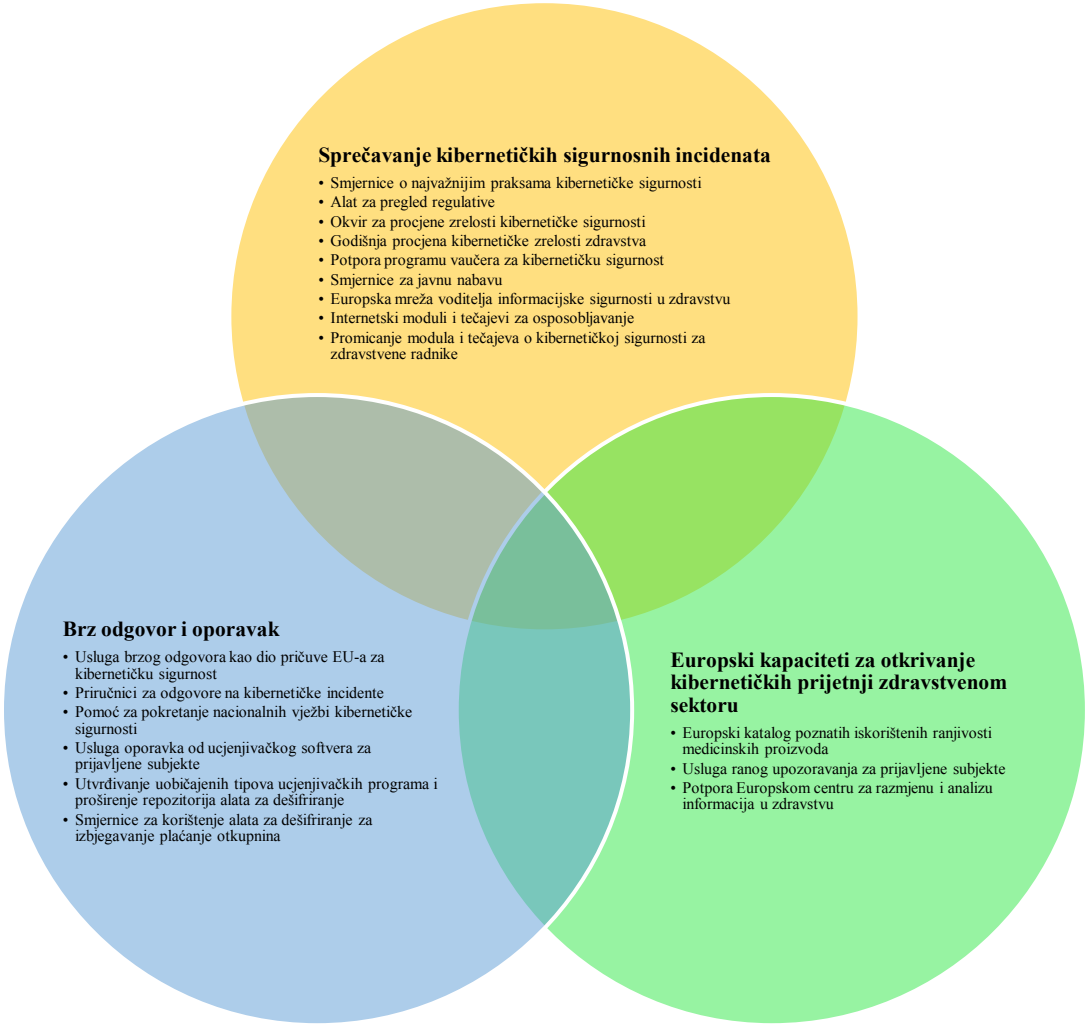
[22] ENISA: *NIS Investments Report 2022* (studeni 2022.). Dostupno na https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

[24] U ovom se dokumentu u istom značenju još koristi „potporni centar”.

trebao bi provoditi u odgovarajućoj koordinaciji s državama članicama, a prioritete i konkretne mjere određivati prema potrebi u stvarnom vremenu.

Kao važan element u izradi kataloga usluga potpornog centra, Komisija će predložiti da se u EU-u pokrenu pilot-projekti kojima će se ustanoviti najbolji načini kibernetičke higijene i procjene sigurnosnih rizika i odgovoriti na potrebu za korištenjem najsuvremenijih kibernetičkosigurnosnih rješenja za kontinuirano praćenje kibernetičke sigurnosti, prikupljanje podataka o prijetnjama i odgovaranje na incidente. Rezultati tih pilot-projekata, koji će se financirati iz programa Digitalna Europa, a provodit će ih Europski stručni centar u području kibernetičke sigurnosti (ECCC), bit će temelj za daljnje mjere na razini EU-a, uključujući rad potpornog centra.



Slika 1: Koncepti za katalog usluga potpornog centra za bolnice i pružatelje zdravstvene zaštite

3.1. Sprečavanje kibernetičkih sigurnosnih incidenata

Jednostavne mjere za bolje izglede

Prema jednoj procjeni osnovne mjere kibernetičke sigurnosti, kao što su redovito ažuriranje sustava, upravljanje sigurnosnim kopijama i uvođenje višestruke autentifikacije, mogu zaštititi organizacije čak od 98 % napada[25]. Mnoge najdjelotvornije mjere kibernetičke higijene i upravljanja rizicima razmjerno je lako uvesti, pa su najlakši izbor za povećanje kibernetičke sigurnosti. Zato bi jedna od glavnih uloga potpornog centra trebala biti **izrada jasnih, ciljanih smjernica s najvažnijim praksama kibernetičke sigurnosti i uputama pružateljima zdravstvene zaštite kako da ih provode**. Taj oblik potpore ne smije biti namijenjen samo velikim bolnicama, nego treba obuhvaćati i savjete prilagođene manjim subjektima, kao što su lokalne ordinacije opće medicine i specijalizirane klinike, koji često nemaju dovoljno resursa da bi imali posebne timove za kibernetičku sigurnost, ali su jednako osjetljivi na napade. Mora se voditi računa i o regionalnoj važnosti koju za skrb o pacijentima imaju pojedini zdravstveni subjekti, primjerice u rijetko naseljenim područjima. Smjernice o osnovnim mjerama kibernetičke sigurnosti mogle bi u povećanju otpornosti pomoći i institutima za zdravstvena istraživanja, koji obrađuju velike količine osjetljivih osobnih podataka.

Zdravstvene organizacije također su dužne ispunjavati niz obveza koje se odnose na kibernetičku sigurnost a proizlaze iz propisa EU-a[26]. Te su obveze ključne za postizanje visoke zajedničke polazne razine kibernetičke sigurnosti i sigurnosti podataka, međutim bitno je da regulatorno okruženje ne bude nepotrebno zahtjevno i zamršeno. Važnost ispunjavanja obveza ne bi smjela biti nauštrb cilja poticanja jake kulture kibernetičke sigurnosti. **Lako dostupan alat za pregled regulative može pomoći da se administrativno opterećenje subjekata na koje se primjenjuje više regulatornih instrumenata**

[25] *Microsoft Digital Defense Report 2022.* Dostupno na https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Kao što je Direktiva NIS 2; Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima (Akt o kibernetičkoj otpornosti) https://eur-lex.europa.eu/eli/reg/2024/2847/oj/hrvhttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/hrv; Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima https://eur-lex.europa.eu/eli/reg/2017/745/oj/hrv https://eur-lex.europa.eu/eli/reg/2017/745/oj/hrvhttps://eur-lex.europa.eu/eli/reg/2017/745/oj/hrv; Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima (Akt o kibernetičkoj otpornosti) https://eur-lex.europa.eu/eli/reg/2017/746/oj/hrvhttps://eur-lex.europa.eu/eli/reg/2017/746/oj/hrv; Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća uredba o zaštiti podataka), https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32016R0679; Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji), https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32024R1689;; Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o europskom prostoru za zdravstvene podatke, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:52022PC0197. Pregovori su završili političkim dogovorom u proljeće 2024., a objava u Službenom listu očekuje se u proljeće 2025. nakon finalizacije.

svede na najmanju moguću mjeru. Uz druge smjernice i pakete alata koje će razviti, potporni centar trebao bi, u bliskoj suradnji s Komisijom i državama članicama, što prije izraditi i proširiti takav alat. Potporni centar imao bi, dakle, važnu ulogu u olakšavanju tumačenja i provedbe propisa o kibernetičkoj sigurnosti, primjerice davanjem provedbenih smjernica[27] i, prema potrebi, promicanjem relevantnih normi.

Buduće **europske lisnice za digitalni identitet** još su jedno sredstvo koje olakšava jednostavnu provedbu dobrih praksi kibernetičke higijene. Naime, da bi se smanjio rizik od neovlaštenog pristupa zdravstvenim podacima, bitno je manje se oslanjati na nepouzdane mehanizme identifikacije kao što su lozinke. Zato je ključno prijeći na sigurne načine prijavljivanja koji se temelje na pouzdanoj identifikaciji. EU-ova lisnica za digitalni identitet pouzdano je, zajedničko rješenje koje će od kraja 2026. zdravstvenim radnicima nuditi usklađenu mogućnost elektroničke identifikacije u cijelom EU-u. Od kraja 2027. svi internetski zdravstveni informacijski sustavi u koje se mora implementirati pouzdana autentifikacija korisnika morat će prihvaćati lisnicu za potrebe identifikacije[28].

Pripravnost i ciljana potpora

Testiranje pripravnosti, što obuhvaća postupke kao što je penetracijsko testiranje, jedan je od temelja dobre kibernetičke sigurnosti. Komisija je ENISA-i već dodijelila sredstva za pilot-inicijative za pripravnost, koje su pokazale da je zdravstveni sektor jedno od područja u kojima se najviše traže testiranja i daljnje procjene kako bi se utvrdile manjkavosti u zrelosti kibernetičke sigurnosti. Stupanjem na snagu Akta o kibernetičkoj solidarnosti te će se aktivnosti znatno povećati, a ECCC će preuzeti vodeću ulogu. Kako bi odgovorila na tu potrebu, Komisija će, nakon savjetovanja sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava (Skupina za suradnju NIS), mrežom EU-CyCLONe[29] i ENISA-om, predložiti da se zdravstvo svrsta među sektore kojima se može dati potpora za **koordinirano testiranje pripravnosti** u skladu s Aktom o kibernetičkoj solidarnosti. Nadalje, potporni centar trebao bi izraditi **prilagođeni okvir za procjene zrelosti kibernetičke sigurnosti u zdravstvenoj zaštiti**. Te bi procjene zrelosti subjektima dale uvide u ranjivosti na temelju kojih bi mogli reagirati i omogućile im da pacijentima i dionicima demonstriraju svoju kibernetičkosigurnosnu pripravnost, što bi povećalo povjerenje u njihove usluge. Na skupnoj razini potporni centar trebao bi provoditi **godišnju procjenu kibernetičke zrelosti zdravstva**, kojom bi dao jasan pregled kibernetičke sigurnosti zdravstvenog sektora na razini država i EU-a.

Zdravstveni sektor se za usluge kibernetičke sigurnosti uvelike oslanja na vanjske izvođače[30], što ukazuje na potrebu za ciljanom potporom jačanju obrane. Vodeći se uspješnim inicijativama kao što su inovacijski vaučeri EU-a, **države članice trebale bi razmotriti ciljane mjere kao što su vaučeri za kibernetičku sigurnost za mikrobolnice, male i srednje bolnice i pružatelje zdravstvene zaštite**. Tim

[27] Izrada smjernica za tumačenje Opće uredbe o zaštiti podataka (GDPR) u nadležnosti je Europskog odbora za zaštitu podataka (EDPB) i ENISA bi pri izradi smjernica trebala potpuno poštovati njegove ovlasti.
[28] Članak 5.f stavci 1. i 2. Uredbe (EU) br. 910/2014.
[29] Europska mreža organizacija za vezu za kibernetičke krize.
[30] Vidjeti ENISA-ino izvješće *NIS Investments Report 2023* (studeni 2023.), u kojem je istaknuta važnost vanjske potpore reviziji i sukladnosti kibernetičke sigurnosti. Dostupno na https://www.enisa.europa.eu/publications/nis-investments-2023.

bi se vaučerima davala financijska pomoć za uvođenje određenih mjera kibernetičke sigurnosti. Prednost pri dodjeli vaučera trebalo bi odrediti prema rezultatima testiranja pripravnosti i procjena zrelosti.

Za uspješno uvođenje vaučera ili drugih programa potpore bitno je uvažiti lokalne okolnosti i lokalno znanje jer se tako postiže njihova relevantnost i dostupnost. Fondovi EU-a, kao što je Europski fond za regionalni razvoj, već podupiru inicijative u području kibernetičke sigurnosti i digitalnog zdravstva, pa bi se mogli iskoristiti za razvoj ciljanih programa vaučera za kibernetičku sigurnost za pružatelje zdravstvene zaštite. Da se to pospješi, potporni centar podupirao bi razvoj takvih regionalnih vaučerskih programa u suradnji s državama članicama i tijelima zaduženima za regionalne programe, oslanjajući se pritom na iskustva iz postojećih nacionalnih projekata kao i mjera financiranih u okviru programa Digitalna Europa kako bi provedba tih programa bila praktična i uspješna.

Uz to, programi Obzor od 2014. imaju važnu ulogu u financiranju niza istraživačkih inicijativa za povećanje otpornosti zdravstvenih ustanova, npr. bolnica, na kibernetičke prijetnje i za smanjenje rizika od zloupotrebe novih tehnologija. Među rezultatima tih inicijativa su razni specijalizirani alati, okviri i sustavi, kao što su alati za procjenu rizika, platforme za dijeljenje podataka koje štite privatnost, kriptografska rješenja, programi informiranja o kibernetičkoj sigurnosti i sustavi za otkrivanje prijetnji u stvarnom vremenu. Važno je reći da se ta rješenja rigorozno provjeravaju pokusnim primjenama u stvarnim zdravstvenim okruženjima kako bi bilo sigurno da su djelotvorna i praktična za zaštitu od kibernetičkih prijetnji.

Osiguravanje lanaca opskrbe u zdravstvenoj zaštiti

Upravljanje složenim lancima opskrbe IKT-om, koji obuhvaćaju razne proizvode kao što su povezani medicinski proizvodi, sustavi elektroničkih zdravstvenih zapisa i uredski hardver, jedan je od najvećih izazova u radu zdravstvenih organizacija. Bolnicama i pružateljima zdravstvene zaštite za rad su potrebni pouzdani i sigurni sustavi i usluge IKT-a. Kako bi pomogla u rješavanju kibernetičkih sigurnosnih problema u zdravstvenom sektoru, Skupina za suradnju NIS trebala bi provesti **koordiniranu procjenu sigurnosnih tehničkih i strateških rizika povezanih s lancima opskrbe medicinskim proizvodima i predložiti mjere njihova ublažavanja**[31]. Ta bi skupina prema potrebi trebala surađivati s Koordinacijskom skupinom za medicinske proizvode.

Akt o kibernetičkoj otpornosti nov je i sveobuhvatan okvir kojim se utvrđuju zahtjevi u pogledu kibernetičke sigurnosti za planiranje, projektiranje, razvoj te rukovanje, primjenu zakrpa i izvješćivanje o aktivno iskorištenim ranjivostima za gotovo sve hardverske i softverske proizvode u svakoj fazi lanca vrijednosti[32]. Medicinski proizvodi su vrsta proizvoda koji se koristi u jednom od najosjetljivijih područja našeg društva. Zahtjevi u pogledu kibernetičke sigurnosti tih proizvoda proizlaze iz postojeće

[31] U skladu s člankom 22. Direktive NIS 2.

[32] U prvoj fazi, koja počinje 1. kolovoza 2025., široke kategorije radijske opreme koje nisu obuhvaćene područjem primjene Uredbe o medicinskim proizvodima i Uredbe o *in vitro* dijagnostičkim medicinskim proizvodima morat će pri stavljanju na jedinstveno tržište ispuniti osnovne zahtjeve Direktive o radijskoj opremi koji se odnose na kibernetičku sigurnost. Akt o kibernetičkoj otpornosti počet će se primjenjivati u drugoj fazi, od 11. prosinca 2027.

Uredbe o medicinskim proizvodima i Uredbe o *in vitro* dijagnostičkim medicinskim proizvodima[33]. Te se uredbe trenutačno evaluiraju kako bi se ispitalo je li ih moguće uskladiti i postići bolju sinergiju među njima, što bi rezultiralo pojednostavnjenjem i zajamčilo najsuvremeniju kibernetičku sigurnost.

Nadalje, rezultati procjene rizika trebali bi pomoći zdravstvenim organizacijama da u skladu s Direktivom NIS 2 preispitaju kibernetičkosigurnosne prakse u lancima opskrbe i mogli bi poslužiti kao temelj za izradu novih **smjernica za nabavu**[34]. Te smjernice izrađuje ENISA-in potporni centar i trebale bi pratiti najnovije trendove kao što je premještanje pohranjenih podataka o pacijentima u oblak, što podrazumijeva potrebu da se migracija elektroničkih zdravstvenih podataka u okruženja u oblaku provede na siguran način. Nadalje, nove bi smjernice organizacijama trebale ponuditi praktične načine praćenja lanaca opskrbe, uključujući pružatelje upravljanih sigurnosnih usluga, izvješća o potvrđivanju ili procjene rizika trećih strana.

Kad je riječ o upravljanju osjetljivim zdravstvenim podacima u oblaku, treba poduzeti daljnje korake kako bi se riješili specifični problemi kao što su povećani rizici za sigurnost, privatnost i poslovanje. Stručnjaci preporučuju da se radi jačanja zaštitnih mjera u uslugama računalstva u oblaku primjenjuje „zadana i integrirana sigurnost". U tom se pristupu prednost daje sigurnoj infrastrukturi, proaktivnom upravljanju ranjivostima te kombinaciji državnih i privatnih rješenja u oblaku. Da bi sigurnosne prakse bile pouzdane, važno je i da postoje kontinuirano praćenje, npr. revizije sukladnosti s nacionalnim i međunarodnim normama, i potvrde za pojedinačne dobavljače, npr. certifikati pružatelja sigurnosti.

Kad je riječ o uslugama kao što su infrastruktura kao usluga (IaaS), platforma kao usluga (PaaS) i softver kao usluga (SaaS), provedba sigurnosnih mjera često je prepuštena korisnicima. Međutim, mnoge zdravstvene organizacije nemaju resursa za samostalno ispunjavanje tih zahtjeva. Zato bi **pružatelje usluga računalstva u oblaku trebalo bi poticati da osnovne sigurnosne mjere implementiraju kao standardnu značajku**. Na taj bi se način smanjio rizik od pogrešnih konfiguracija i održala dosljedna zaštita u okruženjima kojima upravljaju korisnici, koji bi se zato osjećali sigurnijima. Uvođenjem zadane osnovne razine sigurnosti nastojala bi se postići ravnoteža između pouzdane zaštite i praktičnosti, što bi omogućilo upotrebljivost u raznim vrstama zdravstvenih organizacija. Na uvođenju bi blisko surađivali pružatelji usluga računalstva u oblaku i zdravstveni sektor, oslanjajući se na najbolje pristupe iz prakse kako bi razvili učinkovita i prilagodljiva rješenja.

Osposobljavanje i razvoj vještina

Radna snaga s potrebnim vještinama važna je za dugoročni održivi rast i konkurentnost u Europi te za visokokvalitetne usluge, uključujući usluge zdravstvene zaštite. Manjak kvalificiranih stručnjaka za kibernetičku sigurnost velik je problem u cijeloj Europi, a procjenjuje se da za zadovoljavanje potreba

[33] Skupina za suradnju u području medicinskih proizvoda izdala je u prosincu 2019. smjernice o kibernetičkoj sigurnosti medicinskih proizvoda, kojima pomaže proizvođačima da ispune zahtjeve iz tih dviju uredbi, točnije njihova Priloga I.: https://ec.europa.eu/docsroom/documents/41863.

[34] Na temelju ENISA-inih smjernica *Procurement Guidelines for Cybersecurity in Hospitals* iz 2020. (veljača 2020.). Dostupno na https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

za radnom snagom u EU-u nedostaje 299 000 stručnjaka[35]. Prema Eurobarometru o kibernetičkim vještinama iz 2024.[36] 81 % poduzeća smatra da su problemi sa zapošljavanjem stručnjaka za kibernetičku sigurnost među glavnim rizicima za potencijalne kibernetičke napade. U sektorima obrazovanja, zdravstva i socijalnog rada na 66 % radnih mjesta u području kibernetičke sigurnosti rade zaposlenici koji su prije radili druge poslove, što ukazuje na hitnu potrebu za prekvalifikacijom i usavršavanjem.

U nastojanju da se taj problem riješi potporni centar trebao bi surađivati s budućim konzorcijem za europsku digitalnu infrastrukturu (EDIC) za vještine u području kibernetičke sigurnosti, koji je predviđen u Komunikaciji Komisije o Akademiji za vještine u području kibernetičke sigurnosti[37]. Njihov bi rad trebao olakšati dijalog među stručnjacima za kibernetičku sigurnost u zdravstvenom sektoru, kao što su voditelji informacijske sigurnosti (CISO). Jedna od potencijalnih mjera bila bi uspostava **europske mreže voditelja informacijske sigurnosti u zdravstvu**, u kojoj bi za početak skupina stručnjaka razmjenjivala i razvijala najbolje prakse, strategije za zadržavanje talenata i rješenja za privlačenje stručnjaka za kibernetičku sigurnost u zdravstveni sektor. Nadalje, u okviru Akademije za vještine u području kibernetičke sigurnosti trebalo bi, uz potporu industrije i akademske zajednice, razviti resurse za povećanje radne snage u području kibernetičke sigurnosti u zdravstvenom sektoru. U tu bi svrhu trebalo poticati dionike iz industrije da se obvežu podupirati unapređenje osposobljavanja u području kibernetičke sigurnosti.

Ljudske pogreške i dalje su jedan od glavnih uzroka kibernetičkih sigurnosnih incidenata u zdravstvu, što ukazuje na to da postoji hitna potreba za sveobuhvatnim osposobljavanjem osoblja i informiranjem o kibernetičkoj sigurnosti. S obzirom na to da se zdravstveni radnici često služe digitalnim alatima, neophodno je da budu upoznati sa sigurnim praksama. Smanjenju rizika mogu uvelike pridonijeti ciljane kampanje osposobljavanja i informiranja. U tu bi svrhu potporni centar trebao surađivati sa zdravstvenim radnicima i pružateljima usluga te bi s pružateljima usluga obrazovanja i osposobljavanja, industrijom, EDIC-om za vještine u području kibernetičke sigurnosti i tijelima država članica trebao izrađivati i propagirati **opsežne i lako dostupne internetske module i tečajeve za osposobljavanje**.

Uvrštavanje modula o digitalnim kompetencijama i kibernetičkoj sigurnosti u obrazovne kurikulume ključno je za izgradnju čvrstog temelja kibernetičke sigurnosti u zdravstvu. U tim bi se modulima trebala obrađivati sektorska pitanja kao što su zaštita podataka o pacijentima i nedostaci sigurnosti medicinskih proizvoda. Pri razvoju tih resursa trebalo bi uzeti u obzir prethodne aktivnosti, kao što su projekt BeWell,

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Platforma za digitalne vještine i radna mjesta.
[36] Brza anketa Eurobarometra br. 547 o kibernetičkim vještinama.
[37] Komunikacija Komisije Europskom parlamentu i Vijeću: Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije („Akademija za vještine u području kibernetičke sigurnosti”). COM(2023) 207 final.

koji se financira u okviru programa Erasmus+[38], i projekt PANACEA, za koji su sredstva osigurana iz programa Obzor 2020[39].

3.2. Europski kapaciteti za otkrivanje kibernetičkih prijetnji zdravstvenom sektoru

Uspješno otkrivanje kibernetičkih prijetnji ključno je za brz odgovor na incidente. Prijeteći akteri mogu raznim tehnikama otežavati otkrivanje neovlaštenog ulaska i tako produljiti trajanje neovlaštenih pristupa sustavu[40]. Bolje sposobnosti otkrivanja prijetnji zato mogu pridonijeti hitrom zaustavljanju kibernetičkih napada. Naprimjer, u napadu ucjenjivačkim softverom na finskog pružatelja usluga psihoterapije Vastaamo u kojem je počinitelj ucjenjivao pacijente čiji su povjerljivi podaci ukradeni, početni se upad dogodio 2018., ali je pružatelj usluge za njega saznao tek 2020.[41]

Učinkovita razmjena informacija i suradnja izuzetno su važne kako bi se u cijeloj Uniji unaprijedilo otkrivanje prijetnji i informiranost o stanju. Timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) imaju važnu ulogu jer primaju izvješća o incidentima, izbjegnutim incidentima i potencijalnim prijetnjama te daju smjernice o mjerama ublažavanja na nacionalnoj razini. Međutim, **države članice itekako se potiču da sve obavijesti o kibernetičkim incidentima u bolnicama i pružateljima zdravstvene zaštite šalju ENISA-inu potpornom centru da se omogući informiranost o stanju na razini EU-a**. U idealnom bi slučaju te obavijesti trebale sadržavati svrhovitu karakterizaciju raznih bitnih dimenzija incidenta, uključujući poznate osnovne ranjivosti, učinke na zdravstvene usluge i nepovoljne posljedice za pacijente. Nadalje, proizvođači medicinskih i *in vitro* dijagnostičkih proizvoda potiču se da na jedinstvenoj platformi za izvješćivanje koju će uspostaviti i kojom će u okviru Akta o kiberotpornosti upravljati ENISA dobrovoljno prijavljuju iskorištene ranjivosti ili ozbiljne kibernetičke incidente koji utječu na sigurnost tih proizvoda, kao i moguće druge ranjivosti, incidente, izbjegnute incidente ili kibernetičke prijetnje koje mogu utjecati na njihov profil rizičnosti.

Na temelju informacija iz tih izvješćâ, kad prestanu biti osjetljive, potporni centar mogao bi, pod pokroviteljstvom ENISA-e, izraditi europski katalog poznatih iskorištenih ranjivosti medicinskih proizvoda, sustava elektroničkih zdravstvenih zapisa te pružatelja IKT opreme i softvera u zdravstvu. Kao pomoć u rješavanju velikih problema s otkrivanjem prijetnji, potporni centar trebao bi uvesti **uslugu ranog upozoravanja za zdravstveni sektor na razini Unije, koja bi davala upozorenja u gotovo stvarnom vremenu**. Ta bi se usluga temeljila na obrađenim podacima dobivenima od CSIRT-ova, zdravstvenih subjekata i proizvođača, iz otvorenih izvora (OSINT) te od drugih relevantnih aktera kao što su kibernetički centri, centri za razmjenu i analizu informacija (ISAC-i) i tijela kaznenog progona. Boljoj informiranosti o stanju također bi pridonijela pojačana suradnja ENISA-e i Agencije Europske

[38] *BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills*. Dostupno na https://bewell-project.eu/.
[39] *PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people*. Dostupno na https://cordis.europa.eu/project/id/826293.
[40] ENISA Health Threat Landscape 2023.
[41] Odluka 1150/161/2021 finske pravobraniteljice za zaštitu podataka.

unije za suradnju tijela za izvršavanje zakonodavstva (Europol), primjerice po pitanju obrazaca kibernetičkog kriminala u zdravstvenom sektoru.

ISAC-i služe kao središnji izvori podataka o kibernetičkim prijetnjama, potiču dvosmjernu razmjenu informacija između javnog i privatnog sektora te promiču izgradnju povjerenja. Potporni centar trebao bi bolje podupirati **Europski centar za razmjenu i analizu informacija u zdravstvu**, i to alatima i razmjenom informacija, sektorskim izvješćima o informiranosti o stanju te održavanjem pouzdane zajednice za taktičku i stratešku suradnju. Države članice trebale bi poticati razvoj nacionalnih ISAC-a u zdravstvu[42]. Te bi centre trebalo poticati i na povezivanje pružatelja zdravstvene zaštite s proizvođačima kako bi se ujednačilo poimanje kibernetičkih sigurnosnih prijetnji, među ostalim u lancu opskrbe, i olakšao dijalog o sigurnom dizajnu proizvoda koji je doista prilagođen stvarnim uvjetima primjene.

3.3. Brz odgovor i oporavak

S obzirom na veliku osjetljivost zdravstvenih podataka pacijenata i potencijalno razorne učinke kibernetičkih napada na zdravstvene usluge, za zaštitu sigurnosti pacijenata od ključne je važnosti brz i učinkovit odgovor na kibernetičke sigurnosne incidente. Ako bolnica ili pružatelj zdravstvene zaštite postane metom kibernetičkog napada, prva je kontaktna točka relevantni nacionalni CSIRT[43]. Njegova je dužnost dati pravodobnu potporu, idealno u prvih 24 sata, kako bi se lakše izašlo na kraj sa značajnim incidentima. Međutim, ako incident premašuje kapacitet CSIRT-a, za pružanje brzog i učinkovitog odgovora trebala bi biti dostupna potpora EU-a.

Pričuva EU-a za kibernetičku sigurnost, uspostavljena Aktom o kibernetičkoj solidarnosti, obuhvaća usluge odgovora na incidente koje daju pouzdani pružatelji upravljanih sigurnosnih usluga kao pomoć u značajnim kibernetičkim sigurnosnim incidentima ili onima velikih razmjera i kod inicijalnog oporavka. Ta je pričuva osmišljena kao dopuna radu CSIRT-ova država članica koja im omogućuje da zatraže dodatnu potporu u slučajevima kad je pogođen kritični sektor kao što je zdravstvo. Radi poboljšanja tog sustava **Komisija i ENISA trebale bi se pobrinuti da pričuva obuhvaća uslugu brzog odgovora posebno namijenjenu zdravstvenom sektoru**. Ta bi usluga bila dopuna drugim postojećim okvirima te bi, u slučaju nedostatne nacionalne potpore, bez odgode angažirala stručnjake za upravljanje značajnim kibernetičkim sigurnosnim incidentima ili onima velikih razmjera u zdravstvu.

Kako bi se poboljšali odgovor i oporavak, potporni bi centar, u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava, mrežom CSIRT-ova i, prema potrebi, Europolom, trebao izraditi **priručnike za odgovore na kibernetičke incidente prilagođene zdravstvenom sektoru**. Oni bi CSIRT-ove i zdravstvene organizacije usmjeravali u odgovorima na određene kibernetičke

[42] Naprimjer, Finska ima nacionalni ISAC za sektor socijalne i zdravstvene skrbi. Vidjeti Finski nacionalni centar za kibernetičku sigurnost: „*ISAC information sharing groups*", dostupno na https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Člankom 23. stavkom 1. Direktive NIS 2 utvrđuje se zahtjev da ključni i važni subjekti o ozbiljnim incidentima obavješćuju relevantne CSIRT-ove ili, ako je to primjenjivo, nadležno tijelo.

sigurnosne prijetnje, uključujući prijetnje ucjenjivačkim softverom. S obzirom na važnost učinkovite suradnje CSIRT-ova i tijela za izvršavanje zakonodavstva u odgovoru na kibernetičke incidente kriminalne prirode i njihovu istraživanju, priručnici bi, među ostalim, trebali sadržavati jasne smjernice o izvješćivanju tih tijela o takvim incidentima. Nadalje, potporni centar mogao bi **na temelju iskustava iz vježbi kao što je ENISA-ina vježba Cyber Europe 2022. olakšati široko uvođenje nacionalnih vježbi kibernetičke sigurnosti radi testiranja priručnika i usavršavanja protokola za odgovor na incidente**.

Da bi se moglo oblikovati politike i procjenjivati djelotvornost mjera protiv napada ucjenjivačkim softverom, nužno je prikupiti dodatne podatke. U tu bi svrhu države članice trebale od subjekata na koje se primjenjuje Direktiva NIS 2, uključujući zdravstvene organizacije, zatražiti da uz informacije koje dostavljaju kad izvješćuju o značajnim kibernetičkim sigurnosnim incidentima izvijeste i o svim plaćenim otkupninama i otkupninama koje namjeravaju platiti. Takvo izvješćivanje pridonosi učinkovitim istragama incidenata s ucjenjivačkim softverom jer, među ostalim, olakšava praćenje plaćanja na platformama za razmjenu kriptovaluta radi identifikacije primatelja.

Brzina oporavka važan je čimbenik za održavanje otpornosti i povjerenja javnosti, prije svega u zdravstvu, gdje prekid rada može poremetiti skrb o pacijentima. Da bi se mogli uspješno oporaviti od napada ucjenjivačkim softverom, pružatelji zdravstvene zaštite moraju imati sigurne, ažurirane i izolirane sigurnosne kopije koje se mogu brzo staviti u upotrebu. U svojem katalogu usluga potporni centar mogao bi ponuditi **uslugu oporavka od ucjenjivačkog softvera za prijavljene subjekte u okviru koje bi se bolnicama i pružateljima zdravstvene zaštite pomoglo da unaprijed pripreme planove oporavka**. ENISA i Europol trebali bi surađivati na utvrđivanju najčešćih tipova ucjenjivačkog softvera čija su meta zdravstvene organizacije i **proširiti repozitorij alata za dešifriranje** koji su dostupni u okviru projekta No More Ransom[44]. Također bi trebali izraditi i promicati pristupačne smjernice koje će pružateljima zdravstvene zaštite pomoći da koriste alate za dešifriranje kako bi izbjegli plaćanje otkupnina.

Međunarodna inicijativa o suzbijanju napada ucjenjivačkim softverom[45] koristan je forum za razmjenu informacija o pojedinim incidentima s ucjenjivačkim softverom i za izgradnju kapaciteta zemalja članica da učvrste svoje okvire za kibernetičku sigurnost i povećaju sposobnosti za istrage protiv aktera koji koriste ucjenjivački softver. Komisija će u suradnji s Visokom predstavnicom nastaviti unapređivati suradnju u okviru te inicijative, među ostalim u borbi protiv prijetnji ucjenjivačkim softverom zdravstvenom sektoru. Nadalje, Komisija će poticati suradnju u okviru **Radne skupine za kibernetičku sigurnost skupine G-7** u cilju jačanja kibernetičke sigurnosti zdravstvenog sektora. Konkretno, ta bi radna skupina mogla razmotriti mogućnosti za potporu zdravstvenom sektoru u borbi protiv prijetnji, npr. od ucjenjivačkog softvera, na temelju stajališta kao što je Zajednička izjava o napadima ucjenjivačkim softverom na zdravstvene objekte od 8. studenog 2024., koja je iznijeta u okviru Vijeća sigurnosti Ujedinjenih naroda[46].

[44] https://www.nomoreransom.org/en/index.html.
[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

4. Nacionalne mjere

Potencijal ovog akcijskog plana za poboljšanje kibernetičke sigurnosti u zdravstvenom sektoru ovisi o aktivnom sudjelovanju i predanosti država članica. U cilju njegove uspješne provedbe države članice mogle bi imenovati **nacionalne potporne centre za kibernetičku sigurnost posebno namijenjene bolnicama i pružateljima zdravstvene zaštite**. Ti bi centri bili glavne kontaktne točke za zdravstveni sektor na nacionalnoj razini i blisko bi surađivali s ENISA-inim potpornim centrom. Ako je to moguće i relevantno, države članice trebale bi kao nacionalne potporne centre za kibernetičku sigurnost imenovati postojeća tijela, kao što su nacionalni CSIRT-ovi za zdravstvo ili relevantna tijela.

Države članice potiču se i na izradu **nacionalnih akcijskih planova za kibernetičku sigurnost u zdravstvenom sektoru**. U tim bi se planovima opisali specifični kibernetički sigurnosni rizici s kojima se suočavaju zdravstveni sustavi i nacionalne mjere koje se poduzimaju za njihovo suzbijanje te uredilo da se europski resursi i postupci učinkovito primjenjuju. ENISA-in potporni centar može pomoći u izradi tih planova, uzimajući u obzir postojeće nacionalne planove i koordinirajući rad tako da se resursi i strategije pojedinačnih država članica međusobno nadopunjuju.

Države članice posebnu bi pozornost trebale posvetiti i olakšavanju zajedničkog korištenja resursa među pružateljima zdravstvene zaštite, što bi se moglo postići **zajedničkom nabavom ili udruživanjem resursa** na nacionalnoj, regionalnoj ili čak europskoj razini. Tim bi se pristupom smanjilo financijsko opterećenje pojedinačnih subjekata i povećala njihova moć pregovaranja s pružateljima usluga kibernetičke sigurnosti.

Naprimjer, u okviru francuskog programa CaRE[47] na nacionalnoj je i regionalnoj razini uveden niz mjera za lakši pristup resursima: sastavljen je kibernetički katalog s pregledom kibernetičkih rješenja i paketa koji su bolnicama dostupni preko nacionalne agencije za kibernetičku sigurnost, agencije za digitalno zdravstvo, regionalnih agencija i nacionalnih organizacija za nabavu te u okviru komercijalnih rješenja. Uz to, regionalne agencije mogu ponuditi zajedničke resurse za koje mogu iskoristiti dodatno financiranje.

Države članice trebale bi pokušati riješiti i pitanje nedovoljnog ulaganja u kibernetičku sigurnost u zdravstvenom sektoru. Da bi se osigurala odgovarajuća sredstva, trebale bi utvrditi **neobvezujuće referentne vrijednosti i pratiti ciljeve financiranja namijenjenog kibernetičkoj sigurnosti**, vodeći pritom računa da ta ulaganja nemaju nepoželjne posljedice za osnovnu skrb za pacijente. Tim bi ciljevima također trebalo nastojati uključiti pitanja sigurnosti u sva ulaganja u digitalizaciju sektora. Države članice

[47] Francuska agencija za digitalno zdravstvo: *Cybersécurité acceleration et Résilience des Établissements (CaRE)*. Dostupno na https://esante.gouv.fr/strategie-nationale/cybersecurite.

mogu razmjenjivati primjere dobre prakse i savjete o tim ciljevima na platformama kao što je mreža e-zdravstva[48].

5. Suradnja javnog i privatnog sektora

Suradnja javnog i privatnog sektora i savjetovanje s pružateljima zdravstvene zaštite, drugim subjektima u zdravstvenom sektoru i relevantnim akterima u sektoru kibernetičke sigurnosti ključni su za uspješnu provedbu akcijskog plana. Kako bi dodatno pridonijela radu potpornog centra, **Komisija će, uz potporu ENISA-e, osnovati zajednički savjetodavni odbor za kibernetičku sigurnost u zdravstvu** s visokorangiranim predstavnicima iz oba područja, zdravstva i kibernetičke sigurnosti, koji može savjetovati Komisiju i potporni centar o djelotvornim mjerama i razmatrati daljnji razvoj javno-privatnih partnerstava u tom području. Odbor će se oslanjati na dosadašnji rad na uspostavi javno-privatnih partnerstava, uključujući Europski centar za razmjenu i analizu informacija u zdravstvu.

Nadalje, Komisija će **pozvati** poduzeća iz sektora kibernetičke sigurnosti, zaklade, obrazovne ustanove i dionike iz industrije **da se obvežu na poduzimanje mjera za rješavanje problema u tom sektoru**. S obzirom na iskustvo s Akademijom za vještine u području kibernetičke sigurnosti, te bi obveze mogle biti u okviru te akademije i uključivati održavanje tečajeva i izradu materijala za osposobljavanje stručnjaka za kibernetičku sigurnost s težištem na zdravstvenom sektoru[49]. Druge obveze mogle bi se odnositi na aktivnosti informiranja ili pružanje upravljanih sigurnosnih usluga posebno ranjivim subjektima besplatno ili po sniženim cijenama kako bi se povećala njihova pripravnost i otpornost u području kibernetičke sigurnosti. Nadalje, obveze bi mogle obuhvaćati razmjenu podataka o kibernetičkim prijetnjama s ENISA-inim potpornim centrom. Potporni centar trebao bi imati pregled nad obvezama preuzetima u okviru poziva na djelovanje kako bi one bile usklađene i komplementarne.

6. Odvraćanje aktera kibernetičkih prijetnji

Unutarnje i vanjske politike EU-a u području kibernetičke sigurnosti trebale bi podupirati cilj odvraćanja aktera kibernetičkih prijetnji od napada na europske zdravstvene sustave. Kibernetički napadi na zdravstvene organizacije posebno su neprihvatljiva vrsta zlonamjernih kibernetičkih aktivnosti jer mogu ugroziti sigurnost pacijenata i ljudske živote. Stoga treba potpuno iskoristiti kapacitete EU-a za odvraćanje u području kibernetičke sigurnosti i izvršavanja zakonodavstva da se oslabi opći poslovni model aktera prijetnji u zdravstvenom sektoru i da ih se onemogući da lako dolaze do novca. To bi uključivalo olakšavanje prekograničnih istraga boljom razmjenom pokazatelja ugroženosti i drugih relevantnih podataka i pomnije praćenje meta visoke vrijednosti i glavnih posrednika u kaznenim djelima kao što su tzv. neprobojni smještaj na poslužiteljima bez kontrole sadržaja ili kriptomikseri.

[48] Mreža e-zdravstva dobrovoljna je mreža nacionalnih tijela nadležnih za e-zdravstvo koja su imenovale države članice, a uspostavljena je na temelju članka 14. Direktive 2011/24/EU.
Akademija za vještine u području kibernetičke sigurnosti: Uključite se| Platforma za digitalne vještine i radna mjesta.

Instrumenti za kibernetičku diplomaciju okvir su za sprečavanje, odvraćanje i odgovor na kibernetičke napade na EU, države članice i partnere. Visoka predstavnica nastavit će kao odgovor na prijetnje zdravstvenim sustavima primjenjivati postojeći okvir za kibernetičke sankcije.

Kažnjavanje kriminalnih aktera za njihove postupke važan je odvraćajući faktor. Države članice stoga bi se trebale pobrinuti da kazneni progon bude potpuno integriran u njihove nacionalne akcijske planove. Svakako bi trebale u cijelosti iskoristiti odredbe Direktive o napadima na informacijske sustave[50] i Budimpeštanske konvencije Vijeća Europe o kibernetičkom kriminalu za odvraćanje od napada, privođenje kriminalaca pravdi i uništavanje kriminalnih infrastruktura koje olakšavaju napade[51]. Uspješna primjena tih instrumenata trebala bi rezultirati kažnjavanjem kaznenih i zlonamjernih radnji protiv zdravstva.

7. Provedba i praćenje akcijskog plana

Potpornom centru koji će se osnovati u okviru ENISA-e u ovom je akcijskom planu dodijeljen niz zadaća. Na taj se način jamči cjelovita i dosljedna provedba akcijskog plana te se izbjegavaju eventualna preklapanja i dodatni troškovi koji bi mogli nastati osnivanjem novih subjekata. Komisija namjerava osigurati odgovarajuća sredstva za potporni centar.

Nakon što potporni centar počne s radom, ENISA bi, uz savjetovanje s Komisijom, trebala redovito dostavljati najnovije informacije o njegovu radu Upravnom odboru ENISA-e i relevantnim mrežama država članica, prije svega Skupini za suradnju u području sigurnosti mrežnih i informacijskih sustava, mreži CSIRT-ova, mreži e-zdravstva i, prema potrebi, Odboru za europski prostor za zdravstvene podatke. Nadalje, ENISA bi s javno-privatnim savjetodavnim odborom za kibernetičku sigurnost u zdravstvu trebala kontinuirano razmjenjivati informacije o provedbi mjera za koje je zadužen potporni centar.

Redovita izvješća ENISA-e, kao što je Izvješće o stanju kibernetičke sigurnosti u Uniji, koje sadržava objedinjenu procjenu razine zrelosti kibernetičkosigurnosnih kapaciteta i resursa u cijelom EU-u, među ostalim u zdravstvenom sektoru, trebala bi poslužiti kao prilika za objavu relevantnih podataka i pridonijeti praćenju akcijskog plana. Nadalje, ENISA-in indeks kibernetičke sigurnosti EU-a[52] može dati kvantitativne i kvalitativne podatke koji će poslužiti kao dokazna osnova za procjenu kritičnosti i zrelosti zdravstvenog sektora.

8. Sljedeći koraci

[50] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP: https://eur-lex.europa.eu/eli/dir/2013/40/oj/hrv.
[51] Konvencija o kibernetičkom kriminalu (Budimpeštanska konvencija, ETS br. 185) i njezini protokoli: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[52] ENISA, Indeks kibernetičke sigurnosti EU-a, Okvir i metodološka bilješka (2024). Dostupno na https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

U ovoj je Komunikaciji utvrđen ambiciozan program za veću kibernetičku sigurnost zdravstvenog sektora u Europskoj uniji. U akcijskom planu predloženo je da se u okviru ENISA-e osnuje potporni centar za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite te je zacrtan put prema stvaranju usklađenog i zajedničkog europskog pristupa pitanjima kibernetičke sigurnosti u tom sektoru.

Ovu bi Komunikaciju trebalo smatrati prvim korakom u procesu povećanja kibernetičke sigurnosti zdravstvenog sektora. Nakon donošenja akcijskog plana stoga će se pokrenuti sveobuhvatna savjetovanja s dionicima i nastaviti dijalog s državama članicama i relevantnim mrežama radi prikupljanja uvida. Na temelju rezultata savjetovanja Komisija u četvrtom tromjesečju 2025. namjerava iznijeti preporuke za daljnje poboljšanje akcijskog plana.

Komisija poziva države članice i sve dionike da surađuju na ostvarivanju njegovih ciljeva.

PRILOG – Pregled predloženih mjera

Komisija će:

ENISA-in Europski potporni centar za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite	
Osigurati odgovarajuće resurse za potporni centar za kibernetičku sigurnost Surađivati s ECCC-om na pokretanju pilot-projekata za razvoj dobrih praksi kibernetičke higijene i procjene sigurnosnih rizika te na kontinuiranom praćenju kibernetičke sigurnosti, prikupljanju informacija o prijetnjama i odgovaranju na incidente s pomoću najsuvremenijih rješenja kibernetičke sigurnosti, i to u cilju izrade kataloga usluga Europskog potpornog centra za kibernetičku sigurnost	2025.
Sprečavanje kibernetičkih sigurnosnih incidenata	
Na temelju savjetovanja sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava (Skupina za suradnju NIS), mrežom EU-CyCLONe i ENISA-om istražiti mogućnost uvrštavanja zdravstva među sektore kojima se može dati potpora za koordinirano testiranje pripravnosti u skladu s Aktom o kibernetičkoj solidarnosti	Prvo tromjesečje 2025.
Brz odgovor i oporavak	
Zajedno s ENISA-om pobrinuti se da u okviru pričuve EU-a za kibernetičku sigurnost bude dostupna usluga brzog odgovora posebno namijenjena zdravstvenom sektoru	Četvrto tromjesečje 2025.
Suradnja javnog i privatnog sektora	
Uz potporu ENISA-e osnovati zajednički savjetodavni odbor za kibernetičku sigurnost u zdravstvu	Prvo tromjesečje 2025.
Pozvati poduzeća iz sektora kibernetičke sigurnosti, zaklade, obrazovne ustanove i dionike iz industrije da se obvežu na poduzimanje mjera za rješavanje problema u zdravstvenom sektoru	Drugo tromjesečje 2025.
Odvraćanje aktera kibernetičkih prijetnji	
Zajedno s Visokim predstavnikom ispitati mogućnost primjene mjera iz paketa instrumenata za kibernetičku diplomaciju u svrhu sprečavanja zlonamjernih	2025.

aktivnosti protiv zdravstvenih sustava, odvraćanja od njih i odgovora na njih	
U suradnji s Visokom predstavnicom unapređivati međunarodnu suradnju protiv aktera koji koriste ucjenjivački softver, posebno u okviru Međunarodne inicijative o suzbijanju napada ucjenjivačkim softverom	2025. – 2026.
Poticati suradnju u okviru Radne skupine za kibernetičku sigurnost skupine G-7 u cilju jačanja kibernetičke sigurnosti zdravstvenog sektora	2025. – 2026.
Sljedeći koraci	
Provesti sveobuhvatna savjetovanja s dionicima	Prvo tromjesečje 2025.
Donijeti preporuke za daljnje poboljšanje akcijskog plana	Četvrto tromjesečje 2025.

ENISA će:

Potporni centar EU-a za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite	
Započeti s radom na osnivanju Europskog potpornog centra za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite	Drugo tromjesečje 2025.
Izraditi sveobuhvatni katalog usluga koje će pružati potporni centar za kibernetičku sigurnost	Od četvrtog tromjesečja 2025.
Sprečavanje kibernetičkih sigurnosnih incidenata	
Izdati smjernice s najvažnijim praksama kibernetičke sigurnosti i pomagati pružateljima zdravstvene zaštite u njihovoj provedbi	Treće tromjesečje 2025.
U bliskoj suradnji s Komisijom i državama članicama izraditi alat za pregled regulative	Prvo tromjesečje 2025.
Izraditi okvir za procjene zrelosti kibernetičke sigurnosti u zdravstvenoj zaštiti	Treće tromjesečje 2025.
Provoditi godišnju procjenu kibernetičke zrelosti zdravstva	2025. – 2026.
Surađivati s državama članicama i regionalnim programskim tijelima na izradi oglednih programa vaučera za kibernetičku sigurnost	2025. – 2026.

Izraditi nove smjernice za javnu nabavu za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite	Treće tromjesečje 2025.
Osnovati europsku mrežu voditelja informacijske sigurnosti u zdravstvu	Prvo tromjesečje 2026.
Osmisliti i promicati module i tečajeve osposobljavanje zdravstvenih radnika	Prvo tromjesečje 2026.
Europski kapaciteti za otkrivanje kibernetičkih prijetnji zdravstvenom sektoru	
Izraditi europski katalog poznatih iskorištenih ranjivosti medicinskih proizvoda, sustava elektroničkih zdravstvenih zapisa te pružatelja IKT opreme i softvera u zdravstvu.	Četvrto tromjesečje 2025.
Uvesti uslugu ranog upozoravanja za zdravstveni sektor na razini EU-a	Od 2026.
Podupirati Europski centar za razmjenu i analizu informacija u zdravstvu alatima i razmjenom informacija	2025. – 2026.
Brz odgovor i oporavak	
Zajedno s Komisijom pobrinuti se da u okviru pričuve EU-a za kibernetičku sigurnost bude dostupna usluga brzog odgovora posebno namijenjena zdravstvenom sektoru	Četvrto tromjesečje 2025.
U suradnji s mrežom CSIRT-ova izraditi priručnik za odgovor na kibernetičke incidente prilagođen zdravstvenom sektoru	Treće tromjesečje 2025.
Olakšati široko uvođenje nacionalnih vježbi kibernetičke sigurnosti radi testiranja priručnika i usavršavanja protokola za odgovor na incidente	Od četvrtog tromjesečja 2025.
Pružati usluge oporavka od ucjenjivačkog softvera za prijavljene subjekte	Od 2026.
U suradnji s Europolom utvrditi najčešće tipove ucjenjivačkog softvera čija su meta zdravstvene organizacije i proširiti repozitorij alata za dešifriranje u okviru projekta No More Ransom	Četvrto tromjesečje 2025.
U suradnji s Europolom izraditi pristupačne smjernice koje će pružateljima zdravstvene zaštite pomoći da izbjegnu plaćanje otkupnina	Treće tromjesečje 2025.

Nacionalne mjere	
Pomoći državama članicama u izradi nacionalnih akcijskih planova	2025.
Koordinirati rad na postizanju međusobne kompatibilnosti resursa i strategija pojedinih država članica	2025. – 2026.
Provedba i praćenje akcijskog plana	
Uz savjetovanje s Komisijom, relevantnim mrežama država članica redovito dostavljati najnovije informacije o radu potpornog centra za kibernetičku sigurnost	2025. – 2026.
Kontinuirano razmjenjivati informacije sa savjetodavnim odborom za kibernetičku sigurnost u zdravstvu	2025. – 2026.

Države članice će:

Europski kapaciteti za otkrivanje kibernetičkih prijetnji zdravstvenom sektoru	
Europskom potpornom centru za kibernetičku sigurnost prosljeđivati obavijesti o incidentima koje u skladu s Direktivom NIS 2 primaju od bolnica i pružatelja zdravstvene zaštite	Od četvrtog tromjesečja 2025.
Poticati razvoj nacionalnih centara za razmjenu i analizu informacija u zdravstvu	2025. – 2026.
Sprečavanje kibernetičkih sigurnosnih incidenata	
U okviru Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava provesti koordiniranu procjenu sigurnosnih tehničkih i strateških rizika povezanih s lancima opskrbe medicinskim proizvodima	Četvrto tromjesečje 2025.
Brz odgovor i oporavak	
Pokrenuti nacionalne vježbe kibernetičke sigurnosti radi testiranja priručnika i usavršavanja protokola za odgovor na incidente	Od 2026.
Nacionalne mjere	

Imenovati nacionalne potporne centre za kibernetičku sigurnost bolnica i pružatelja zdravstvene zaštite	Drugo tromjesečje 2025.
Izraditi nacionalne akcijske planove za kibernetičku sigurnost u zdravstvenom sektoru	Četvrto tromjesečje 2025.
Olakšati razmjenu resursa među pružateljima zdravstvene zaštite	2025. – 2026.
Utvrditi neobvezujuće referentne vrijednosti i pratiti ciljeve financiranja za kibernetičku sigurnost	Četvrto tromjesečje 2025.
Zatražiti od zdravstvenih organizacija i drugih subjekata na koje se primjenjuje Direktiva NIS 2 da izvješćuju o namjerama plaćanja otkupnina	Četvrto tromjesečje 2025.